Mark C. Mao, CA Bar No. 236165
Sean P. Rodriguez, CA Bar No. 262437
Beko Reblitz-Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
srodriguez@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

William Christopher Carmody
(admitted *pro hac vice*)
Shawn J. Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas,
32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
Ryan J. McGee (admitted *pro hac vice*)
Michael F. Ram (admitted *pro hac vice*)
Ra O. Amen (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com
ramen@forthepeople.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, MARIA NGUYEN, WILLIAM BYATT, JEREMY DAVIS, and CHRISTOPHER CASTILLO, individually and on behalf of all other similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No.: 5:20-cv-03664-LHK

PLAINTIFFS' OPPOSITION TO GOOGLE'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

The Honorable Lucy H. Koh
Courtroom 8 – 4th Floor
Date: February 25, 2021
Time: 1:30 p.m.

TABLE OF CONTENTS

MEMORANDUM OF POINTS AND AUTHORITIES 1

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 3

A. Plaintiffs Never Consented to Google's Interception 3

B. Google Did Not Obtain the Websites' Consent, Either 4

C. Google Now Admits It Intercepts Private Browsing Communications 4

D. Google Associates the Private Browsing Data with Preexisting User Profiles and Sells It to Advertisers for Hundreds of Millions of Dollars 5

ARGUMENT 5

I. Plaintiffs State a Claim Under the Wiretap Act 5

A. Google's Consent Defense Is Meritless 6

1. Plaintiffs Did Not Consent 6

2. Websites Did Not Consent 10

B. Consent Is Irrelevant Because Google Intercepted the Private Browsing Communications with the Intent to Commit a Criminal or Tortious Act 12

1. The FTC Consent Decree 13

2. The California Consumer Privacy Act ("CCPA") 13

3. The Comprehensive Computer Data Access and Fraud Act ("CDAFA") 14

4. Intrusion Upon Plaintiffs' Seclusion and Constitutional Right to Privacy 14

C. The "Ordinary Course of Business" Exception Does Not Apply 15

II. Plaintiffs State Claims Under the California Invasion of Privacy Act 16

III. Plaintiffs State a Claim Under the CDAFA 18

IV. Plaintiffs State Constitutional and Common Law Privacy Claims 20

A. Plaintiffs Had a Reasonable Expectation of Privacy 20

B. Google's Conduct Was "Highly Offensive" 22

V. Plaintiffs' Claims Are Timely 24

VI. CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

Cases

In re Animation Workers Antitrust Litig.,
123 F. Supp. 3d 1175 (N.D. Cal. 2015) (Koh, J.) 24, 25

In re Anthem, Inc. Data Breach Litig.,
No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016) (Koh, J.) 13

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 5

Belluomini v. Citigroup, Inc.,
No. CV 13-01743 CRB, 2013 WL 3855589 (N.D. Cal. July 24, 2013) 22

Bliss v. CoreCivic, Inc.,
No. 19-16167, 2020 WL 6279679 (9th Cir. Oct. 27, 2020) 3, 24

Brodsky v. Apple Inc.,
445 F. Supp. 3d 110 (N.D. Cal. 2020) (Koh, J.) 19

Cain v. State Farm Mutual Auto. Ins. Co.,
62 Cal. App. 3d 310 (1976) 25

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014) 6, 10

In re Carrier IQ,
78 F. Supp. 3d 1051 (N.D. Cal. 2015) 19

Cover v. Windsor Surry Co.,
No. 14-CV-05262-WHO, 2015 WL 4396215 (N.D. Cal. July 17, 2015) 25

Davis v. Facebook, Inc.,
956 F.3d 589 (9th Cir. 2020) ..... *passim*

In re Facebook, Inc., Consumer Privacy User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019) 8

Facebook, Inc. v. Power Ventures, Inc.,
No. C 08-05780 JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010) 18

Flanagan v. Flanagan,
27 Cal. 4th 766 (2002) 16, 17

Folgelstrom v. Lamps Plus, Inc.,
195 Cal. App. 4th 986, 992, 125 (2011) 22

Gonzales v. Uber Technologies, Inc.,
305 F. Supp. 3d 1078, 1092 (N.D. Cal. 2018) 22

In re Google Assistant Privacy Litig.,
457 F. Supp. 3d 797 (N.D. Cal. 2020) 23, 24

In re Google Inc. Cookie Placement Consumer Privacy Litig.,
806 F.3d 125 (3rd Cir. 2015) 21, 23, 24

In re Google Inc. ("Gmail"),
No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) (Koh, J.) ..... *passim*

In re Google, Inc. Privacy Policy Litig.,
58 F. Supp. 3d 968 (N.D. Cal. 2014) 22, 23

Hameed-Bolden v. Forever 21 Retail, Inc.,
No. CV1803019SJOJPRX, 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018) 13

Henry Schein, Inc. v. Cook,
2017 WL 783617 (N.D. Cal. Mar. 1, 2017) 19, 20

In re iPhone Application Litigation,
844 F. Supp. 2d 1040 (N.D. Cal. 2012) (Koh, J.) 22

Kight v. CashCall, Inc.,
200 Cal. App. 4th 1377 (2011) 17

In re Lithium Ion Batteries Antitrust Litig.,
No. 13-MD-2420 YGR, 2014 WL 309192 (N.D. Cal. Jan. 21, 2014) 25

Low v. LinkedIn Corp.,
900 F. Supp. 2d 1010 (N.D. Cal. 2012) (Koh, J.) 22

Manzarek v. St. Paul Fire & Marine Ins. Co.,
519 F.3d 1025 (9th Cir. 2008) 5, 21

Matera v. Google Inc. ("Gmail II"),
No. 15-CV-04062-LHK, 2016 WL 5339806 (N.D. Cal. Sept. 23, 2016) (Koh, J.) 6, 10, 16

In re Maxim Integrated Prod., Inc.,
No. 12-244, 2013 WL 12141373 (W.D. Pa. Mar. 19, 2013) 14

Mirkarimi v. Nevada Prop. 1 LLC,
No. 12CV2160-BTM-DHB, 2013 WL 3761530 (S.D. Cal. July 15, 2013) 16, 17

Moreno v. San Francisco Bay Area Rapid Transit District,
No. 17-CV-02911-JSC, 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017) 22

In re Nickelodeon Cons. Priv. Litig.,
827 F.3d 262 (3d Cir. 2016) 21, 23, 24

O'Shea v. Cty. of San Diego,
No. 19-CV-1243-BAS-BLM, 2020 WL 2767357 (S.D. Cal. May 28, 2020) 25

Opperman v. Path, Inc.,
205 F. Supp. 3d 1064 (N.D. Cal. 2016) 20

People v. Nakai,
183 Cal. App. 4th 499 (2010) 17

Perkins v. LinkedIn Corp.,
53 F. Supp. 3d 1190 (N.D. Cal. 2014) (Koh, J.) 8

In re Pharmatrak, Inc.,
329 F.3d 9 (1st Cir. 2003) 6, 10

Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress,
214 F. Supp. 3d 808 (N.D. Cal. 2016) 15

Plumlee v. Pfizer, Inc.,
No. 13-CV-00414-LHK, 2014 WL 695024 (N.D. Cal. Feb. 21, 2014) 25

Quan v. Smithkline Beecham Corp.,
149 F. App'x 668 (9th Cir. 2005) 25

Revitch v. New Moosejaw, LLC,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) 17, 18

S.D. v. Hytto Ltd.,
No. 18-CV-00688-JSW, 2019 WL 8333519 (N.D. Cal. May 15, 2019) 16

Saling v. Royal,
No. 2:13-CV-1039-TLN-EFB, 2015 WL 5255367 (E.D. Cal. Sept. 9, 2015) 25

Synopsys, Inc. v. Ubiquiti Networks, Inc.,
313 F. Supp. 3d 1056 (N.D. Cal. 2018) 19

United States v. Christensen,
828 F.3d 763 (9th Cir. 2015) 2, 19, 20

In re Vizio, Inc., Consumer Privacy Litig.,
238 F. Supp. 3d 1204 (C.D. Cal. 2017) 24

Watkins v. L.M. Berry & Co.,
704 F.2d 577 (11th Cir. 1983) 10, 12

Wilson v. City of Oakland,
No. C-11-05377 DMR, 2012 WL 669527 (N.D. Cal. Feb. 29, 2012) 25

In re Yahoo Mail Litig.,
7 F. Supp. 3d 1016 (N.D. Cal. 2014) (Koh, J.) 6, 22

Yunker v. Pandora Media, Inc.,
No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) 22

Statutes

18 U.S.C. § 2511(2)(d) 2, 6, 12, 15

18 U.S.C. § 2520(e) 24

Cal. Civ. Code § 1798.100(b) 14

Cal. Civ. Code § 1798.140(o)(1) 14

Cal. Civ. Code § 1798.155 14

Cal. Civ. Proc. Code § 335.1 25

Cal. Civ. Proc. Code § 340(c) 25

Cal. Penal Code § 502(c)(2) 14, 18, 20

Cal. Penal Code § 502(e)(5) 24

Cal. Penal Code § 631(a) 16, 24

Cal. Penal Code § 632(a) 2, 16, 24

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This case arises out of Google's surreptitious interception and collection of data from users who had set their web browser to a "private browsing" mode, including Google's "Incognito" mode. Google never disclosed that it would intercept and collect data from users who were in private browsing mode. Rather, Google explicitly promised that users were in control and had the power to stop Google's data collection by using private browsing mode. Those Google promises were (and still are) false. Google's Motion ("MTD") confirms, as alleged, that Google intercepts and collects data from its users' private browsing communications. In its effort to evade liability, Google now admits that its promises of consumer privacy and control are, and always have been, a ruse. The truth is that users are powerless to stop Google's data collection.

Google's contention that Plaintiffs consented to Google's interception of their private browsing communications is simply false. Plaintiffs did not consent, and they could not have consented since Google concealed what Google was doing. FAC ¶¶ 1, 4, 85, 191, 214. Google repeatedly (and falsely) assured Plaintiffs that they were "in control of what information you share with Google," across all of Google's services, and that they could "browse the web privately" without Google "linking any activity to you." FAC ¶¶ 42, 146. Google never once disclosed that it would intercept Plaintiffs' communications while Plaintiffs were in private browsing mode. FAC ¶¶ 1-4, 42-43. One cannot consent to what one does not know.

Google's contention that *websites* gave consent is equally false. Google never disclosed to websites that Google would intercept users' private browsing communications, and websites never consented to these interceptions. FAC ¶¶ 75-77, 83, 215. Instead, Google represented to websites that it would adhere to Google's own privacy policies, including Google's assurances that Google would not collect data from users in "private browsing" mode. FAC ¶¶ 76, 83. Google only recently (after the filing of this lawsuit) launched a "Consent Mode (Beta)" to address this consent issue. FAC ¶¶ 73, 140. Websites have not consented to Google's interception of private browsing communications. FAC ¶¶ 77, 83.

Consent is also no defense to Plaintiffs' Wiretap Act claim because Google intercepted the private browsing communications for the purpose of violating four other laws. *See* 18 U.S.C. § 2511(2)(d) (consent is not a defense if the "communication is intercepted for the purpose of committing any criminal or tortious act"). Google intercepted Plaintiffs' private communications for the purpose of associating data from those private communications with users' preexisting profiles, further enriching those profiles, and then using those enhanced profiles to generate advertising revenues for Google across multiple websites. FAC ¶¶ 91-93, 104, 108, 113-15. Those subsequent acts by Google constituted independent violations of law. FAC ¶¶ 154-65.

Google's remaining defenses to Plaintiffs' Wiretap Act and California Invasion of Privacy ("CIPA") claims also fail. The "ordinary course of business" exception to the Wiretap Act would only apply "if the alleged interceptions were an instrumental part of the transmission" of the private browsing communications. *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013) (Koh, J.) [hereinafter *Gmail*]. Here, Google's interception of Plaintiffs' private browsing communications was *not* an "instrumental part of the transmission" of those communications—on the contrary, Google's surreptitious interception had no bearing on Plaintiffs' communications with the websites. FAC ¶ 213. And Google's argument that the communications (which Google affirmatively promised would be private) are not "confidential" under CIPA § 632 rests on a misunderstanding of California law and is contrary to the facts alleged.

Plaintiffs have also stated a claim under the Comprehensive Computer Data Access and Fraud Act ("CDAFA"). The Ninth Circuit has rejected the "circumvention" requirement Google attempts to read into the CDAFA. *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015). Even applying that requirement, Plaintiffs' allegations would still be sufficient. Google's "terms of use" defense gets it backwards: Courts decline to hold *users* liable under the CDAFA for exceeding the scope of a website's terms of use. Those authorities have nothing to do with this case, where Google has acted contrary to *its own* privacy policies.

Plaintiffs have also properly alleged constitutional and common law privacy claims. Plaintiffs had a reasonable expectation of privacy, both because of the "sensitive" nature of their

private browsing communications *and* because of the "surreptitious and unseen" nature of Google's interception. *Davis v. Facebook, Inc.*, 956 F.3d 589, 602-04 (9th Cir. 2020). Google's "surreptitious data collection" also amounts to highly offensive conduct. *Id.* at 606. Google responds by raising a factual dispute as to whether it correlates private browsing data with individual users, which is contrary to Plaintiffs' allegations (FAC ¶¶ 92-108, 115) and cannot be resolved on a motion to dismiss. In any event, even if Google were correct about this (it's not), Plaintiffs would still have stated claims because Google "set an expectation that [private browsing] data would not be collected, but then collected it anyway." *Davis*, 956 F.3d at 602.

Finally, Plaintiffs' claims are timely. "[E]ach interception is a discrete violation" that triggers its own statute of limitations. *Bliss v. CoreCivic, Inc.*, No. 19-16167, 2020 WL 6279679, at *3-4 (9th Cir. Oct. 27, 2020). Any applicable statutes of limitations were also tolled because Google's false and misleading statements prevented Plaintiffs from discovering the truth.

II. FACTUAL BACKGROUND

A. Plaintiffs Never Consented to Google's Interception

People care deeply about retaining control over their browsing data. FAC ¶¶ 60, 162. This is particularly important for users' private browsing data, which often reveals sexual interests, political views, and other sensitive, private information. FAC ¶ 162. Recognizing consumers' concerns and expectations of privacy, Google repeatedly and uniformly assured users that they were "in control of what information [they] share with Google" and that users could adjust their privacy settings "across [Google's] services" to "control what [Google] collect[s] and how [their] information is used." FAC ¶¶ 2, 42. To exercise this "control" across Google's services, users were specifically invited by Google to "browse the web privately" by selecting a private browsing mode, including Google Incognito mode and equivalent features on other browsers. FAC ¶ 42. These private browsing modes, according to Google, "let[] you browse the web without linking any activity to you." FAC ¶ 146. When users selected Google's Incognito mode, in Google's Chrome browser, they were automatically taken to a Google pop-up disclosure screen that further assured them that "Chrome won't save . . . your browsing history." FAC ¶ 52. Instead, the

disclosure stated that only three entities, *excluding Google*, "might" be privy to private browsing activity. *Id.* With no disclosure of Google's interception, and relying on Google's representations, Plaintiffs reasonably believed that Google would not keep a record of, or make a use of, their private browsing data. FAC ¶¶ 3, 41-43, 53, 168, 173, 178, 188, 214. Accordingly, Plaintiffs could not have consented to Google's interception of their private browsing communications. FAC ¶¶ 1, 3, 41-43, 85, 191, 214.

B. Google Did Not Obtain the Websites' Consent, Either

Google never obtained consent from websites for its interception of users' private browsing communications. FAC ¶¶ 75, 83. To utilize certain Google services, Google requires websites to embed Google's custom code into their existing code, which are then sent to users' browsers to generate secret, duplicated messages that are sent to Google's servers. FAC ¶¶ 67-68, 78-79. But Google never disclosed to websites that Google intercepts and collects data from private browsing. FAC ¶¶ 73-77. To the contrary, Google assured websites that Google would adhere to its own privacy policies—which include the very same privacy assurances to users that they could "control what [Google] collect[s] and how [their] information is used" across Google's services, by entering "private browsing" mode. FAC ¶¶ 2, 42, 76, 83. Only after the filing of this lawsuit did Google launch a new "Consent Mode (Beta)" feature, which is (Google claims) intended to assist websites to identify whether a particular user has consented to its use of Google Analytics and other Google services. FAC ¶¶ 73, 140.

C. Google Now Admits It Intercepts Private Browsing Communications

Without providing any notice to users or obtaining consent, Google's software scripts (pieces of Google code embedded within websites that use Google for analytics and advertising services) secretly cause users' browsers to send copies of their private browsing communications to Google's servers in California. FAC ¶ 5. When a user visits a webpage, the user's browser sends a GET request to the website, which tells the website precisely what content the user is asking the website to display, as well as a referrer header containing the URL information of what the user has been viewing and requesting from other websites. FAC ¶¶ 5, 63. Google's embedded

code within websites also causes the user's browser to send a duplicate copy of that GET request, along with other browsing information, to Google's servers. FAC ¶¶ 63, 65. Google's duplication and receipt of the user-website GET Request occurs in addition to but concurrent with the transmission of the GET request from the user's browser to the website. FAC ¶ 64. Google now admits it intercepts and collects data from these private browsing communications. MTD at 1-2.

D. Google Associates the Private Browsing Data with Preexisting User Profiles and Sells It to Advertisers for Hundreds of Millions of Dollars

Google maintains "profiles" on its users—collections of information regarding the users' attributes and online history—which Google uses to generate advertising revenues and for other purposes. FAC ¶¶ 89-93, 113-23. After intercepting a user's private browsing communications, Google sets out to identify the user so that it can package the data with the "profile" Google maintains on the user. FAC ¶¶ 89-116. Google profits from the private browsing data it collects because this data enriches Google's profiles on users, which means that Google can charge advertisers and websites more for its services. FAC ¶¶ 115-16. Google also profits because the data improves Google's own algorithms and technology. FAC ¶ 115.

ARGUMENT

A motion to dismiss must be denied if the complaint "state[s] a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* The court must "accept factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

I. Plaintiffs State a Claim Under the Wiretap Act

As alleged and now admitted by Google, Google intercepts private browsing communications. FAC ¶¶ 202-17; MTD at 1-2. Google's primary defense is its meritless contention that Plaintiffs and the websites consented to that interception. MTD at 9.

A. Google's Consent Defense Is Meritless

As in prior cases before this Court, Google has not met its burden of establishing consent. As "'the party seeking the benefit of the exception,' it is Google's burden to prove consent." *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 5339806, at *17 (N.D. Cal. Sept. 23, 2016) (Koh, J.) [hereinafter *Gmail II*] (citation omitted). There is only consent when the disclosure gives users notice of the "specific practice" at issue. *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 847-48 (N.D. Cal. 2014). Here, Google cannot meet its burden because Google never disclosed its interception of private browsing communications. On the contrary, the uniform disclosures that Google cites repeatedly assured users that Google would *not* intercept communications from users in "private browsing" mode. None of the cherry-picked documents submitted by Google provide any support for Google's consent defense.[1]

1. Plaintiffs Did Not Consent

Google's principal argument is that Plaintiffs consented by agreeing to Google's Privacy Policy, which provides that Google "collect[s] information about your activity in our services, . . . includ[ing] . . . [a]ctivity on third-party sites and apps that use our services." MTD at 5; Ex.[2] 1 at 3 (Google Privacy Policy).[3]

However, that provision never mentions private browsing, and it in no way discloses Google's interception of private browsing communications. As detailed in the FAC, Google's Privacy Policy states that private browsing mode (including Incognito mode) prevents Google from collecting the data it typically collects by way of the services it provides to websites:

---

[1] Google's Motion ignores that "consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the interceptions." *Gmail II*, 2016 WL 5339806, at *17. Moreover, "consent under § 2511(2)(d) is 'not an all-or-nothing proposition.'" *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014) (Koh, J.) (quoting *Gmail*, 2013 WL 5423918, at *12). Rather, "a party may consent to the interception of . . . only a subset of its communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003).

[2] Exhibit 1 is attached to the concurrently filed declaration of Amanda Bonn.

[3] Google references an earlier version of the Privacy Policy in its brief but admits that "subsequent versions" [including the one attached here as Ex. 1] "contained identical or substantively identical disclosures." MTD at 6 n.6.

- "[A]cross ***our services***, you can adjust your privacy settings to ***control what we collect*** and how your information is used."
- "You can use ***our services*** in a variety of ways to manage your privacy. For example, . . . [y]ou can [] choose to browse the web privately using Chrome in Incognito mode."
- "***Our services*** include . . . [p]roducts that are integrated into third-party apps and sites, like ads . . . ."

FAC ¶ 42; Ex. 1 at 1 (emphases added). Google's Privacy Policy thus promises users that they can "control what [Google] collect[s]" "across [Google's] services," including services Google provides to websites. Google invites users to exercise that control by choosing to browse privately. A reasonable user would understand that using a private browsing mode prevents Google from collecting the data it typically collects from third-party websites. FAC ¶¶ 3, 41-43, 53.

Other uniform Google disclosures similarly demonstrate a lack of consent, promising that users can "control" what information Google collects by choosing to browse privately:

- "You're in control of what information you share with Google when you search. ***To browse the web privately, you can use private*** browsing . . . ."

FAC ¶ 42. With its promise of "control" and invitation to browse privately, Google assures users that they can "control" the information they "share with Google" by "us[ing] private browsing." Without disclosing its interception and instead promising privacy, users reasonably understood that Google would not intercept private browsing communications. FAC ¶¶ 3, 41-43, 53.

And if there were any doubt (there wasn't), Google's Incognito Screen—a uniform, pop-up disclosure generated when users enter the "private browsing" mode of Google's own Chrome browser—assures users that only three entities, *not including Google*, might view user's activity:

- "Chrome won't save . . . [y]our browsing history [and] [c]ookies and site data."
- "Your activity might still be visible to: the websites you visit, your employer or school, or your internet service provider."

FAC ¶ 52. Google also made numerous statements throughout the Class Period reiterating that it would not view private browsing communications. *See* FAC ¶¶ 42, 146 (listing numerous promises).[4] Nothing in Google's Privacy Policy, or in any other Google disclosure, informed users

[4] *E.g.*, FAC ¶ 42 ("When you have incognito mode turned on in your settings, your search and browsing history will not be saved."); *id.* ¶ 146 (describing "Incognito mode" as "the popular feature in Chrome that lets you browse the web without linking any activity to you").

that Google would continue to intercept, collect, and use their data even when the users entered "private browsing" mode. FAC ¶¶ 44-59.

It is axiomatic that one cannot consent to what one does not know. Google turns this axiom on its head by claiming users somehow consented to a practice Google never disclosed. This Court already rejected a version of this argument in *Gmail*. 2013 WL 5423918, at *13-14. In that case, users alleged that Google illegally intercepted emails to and from Gmail users, and then used those emails to create user profiles and to send targeted advertising. This Court rejected Google's consent defense, reasoning that "[n]othing in the [Privacy] Policies suggests that Google intercepts email communication in transit between users." *Id.* Instead, the policies "obscure[d] Google's intent to engage in such interceptions" by "explicitly stat[ing] that Google collects 'user communications . . . *to Google.*'" *Id.* at *14.

At least as much obfuscation, by Google, is present here as in *Gmail*. In this case, Google's Privacy Policy "obscure[d] Google's intent," *id.*, by stating that users could "control what we collect" and "browse privately" by placing their browsers in "private browsing" mode. FAC ¶ 42. Google's Incognito Screen similarly "obscure[d] Google's intent" by telling users that "*websites*" "might" see Plaintiffs' communications, omitting that Google's embedded code within those websites would also intercept and redirect the communications *to Google*. *See also In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019) (rejecting consent defense because consent was not the "only plausible interpretation").[5]

Google's argument otherwise depends on cutting and pasting together snippets from two *separate documents*, to pretend both documents were presented to users at once. They were not. Google supplements the Incognito Screen with an additional webpage attached to its motion (Exhibit 19) in an effort to make it appear as if the Incognito Screen disclosed more than it truly did. In its motion, Google writes: "[The Incognito Screen] made clear that . . . 'your activity might

[5] Users also have no ability to opt out. FAC ¶ 66; *cf. Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1213 (N.D. Cal. 2014) (Koh, J.) (deeming the plaintiffs to have consented to the conduct at issue in light of their "ability to opt out," and distinguishing *Gmail*, in which "users who sought to use Gmail could not opt out of the allegedly unlawful conduct").

still be visible to' inter alia, 'Websites you visit, *including the ads and resources on those sites*.'" MTD at 10. But the italicized words in Google's MTD are *not* part of the Incognito Screen at the point of collection. Instead, those words come from Exhibit 19—a printout from some other webpage that Google attached to its Motion. Google's Request for Judicial Notice, ECF No. 84, does not tell the Court how Plaintiffs would have accessed Exhibit 19, nor the time period when Exhibit 19 would have been accessible.

In any event, Exhibit 19 does not establish consent either. In Exhibit 19, Google never discloses that "Google" is one of the "ads and resources on" websites that might be privy to private browsing communications. In fact, Exhibit 19 makes no reference to Google at all. The references in Exhibit 19, to "ads and resources on" websites, cannot possibly be understood as telling users that *Google itself* will intercept, collect, and use every single GET request communication by the user to these websites—in addition to other browser information.

Equally unavailing is Google's suggestion that it told users that private browsing mode would *only* conceal their browsing activity from other household members. MTD at 4. Google's statements were not so limited. This family-privacy aspect of private browsing is irrelevant. A user can seek privacy from both their family and from Google—these are not mutually exclusive. The Incognito Screen promises as much, explaining that "Now, you can browse privately, *and* other people who use this device won't see your activity" while never mentioning that Google itself will continue to intercept communications. FAC ¶ 52 (emphasis added).

Finally, Google's repeated focus on the fact that Incognito mode does not share a browser's existing cookies with websites during private browsing sessions is simply irrelevant—Google appears to be litigating some other case entirely. MTD at 6-8 & n.7. Plaintiffs do *not* allege that Google intercepts their private browsing communications through Google cookies. Instead, *Plaintiffs allege that hidden code, embedded within websites that use Google for analytics and advertising services, surreptitiously caused Plaintiffs' browsers to transmit copies of Plaintiffs' communications and other browsing history to Google's servers.* FAC ¶¶ 5, 63-65.

Google's consent defense is contrary to this Court's decisions regarding what constitutes consent. If credited, Google's arguments would destroy consumers' reasonable privacy expectations. Furthermore, Google's consent defense is belied by the numerous cited disclosures, each of which represented that private browsing kept users' activity hidden from Google. FAC ¶¶ 42, 146 (listing statements). If Google continues to intercept communications even while users have enabled private browsing mode, as it now brazenly admits, then what "control" do users have to prevent such interceptions? Google has no answer. Given what Google has said (and not said) about its interception of private browsing communications, Google's recycled consent defense, which this Court already rejected in *Gmail*, should be rejected once more.

2. Websites Did Not Consent

Nor did the recipients of users' private browsing communications (the websites) consent to Google's interception. Here, again, "it is Google's burden to prove consent." *Gmail II*, 2016 WL 5339806, at *17. "Consent . . . is not to be cavalierly implied" as doing so would "thwart" the Wiretap Act's "strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place." *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983). This Court has accordingly "cautioned that implied consent applies only in a narrow set of cases." *Gmail*, 2013 WL 5423918, at *12 (citing *Watkins*, 704 F.2d at 581.). Google cannot meet its burden to show any consent by websites.

Google's principal contention is that websites must have consented because they allowed Google's custom code to be embedded on their websites. MTD at 11. Google's choice of wording is again telling: it argues that the websites impliedly consented to "Google's receipt of the Data *generally*." MTD at 12. But implied consent, like express consent, "is not an all-or-nothing proposition." *Gmail*, 2013 WL 5423918, at *12. "[A] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *Id.* (citing *In re Pharmatrak*, 329 F.3d 9, 19 (1st Cir. 2003)). Here, there is no such consent. *See also Campbell*, 77. F. Supp. 3d at 847-48 (rejecting implied consent defense because the defendant did not establish "consent to the specific practice" being challenged).

As a threshold matter, Google misrepresents the technical process by which Google receives copies of the user-website GET requests. Contrary to Google's description, the embedded Google code does not transmit the data from the websites to Google. Instead, similar to *Davis*, Google's embedded code secretly causes the *user's browser*, not the websites, to send an additional message to Google's servers containing the duplicated GET request. FAC ¶¶ 5, 63; 956 F.3d at 608 (describing identical process). The websites are not directly part of the transmission between the user's browser to Google's server, and therefore the websites could not have consented to that communication. That would be akin to a person (the websites) consenting to a stranger (Google) breaking into another person's home (the user) to listen in on an unauthorized conversation. No lawful consent exists to such circumstances.

In any event, the websites' act of allowing Google to embed Google's code does not address the "critical question," which is whether the websites "had adequate notice of the interception" at issue. *Gmail*, 2013 WL 5423918, at *12. Google provided no such notice to the websites *when users enabled private browsing mode*. FAC ¶¶ 75-76, 83. To the contrary, Google assured websites that Google would always adhere to its own privacy policies, including its promise to allow users to "adjust your privacy settings to control what we collect and how your information is used" and the opportunity "to browse the web privately." FAC ¶¶ 42, 76, 83. The only thing websites consented to was permitting their users to exercise the very privacy controls Google promised, which Google now claims should be construed as meaningless.[6]

Google speculates that the websites must have known that Google had the capability of intercepting the websites' communications with Plaintiffs. MTD at 12. But Google's capabilities are beside the point—websites would not have expected Google to contravene its own privacy policies, even if Google had the capability to do so. Regardless, a website's general awareness of Google's capability is also "insufficient to establish implied consent." *Gmail*, 2013 WL 5423918, at *12. Google does not identify any occasion where it actually informed any website that it would

[6] Google's cited cases on this point are inapposite, decided years before private browsing mode even existed. MTD at 11-12 (citing *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *Chance v. Ave. A*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001)).

intercept private browsing communications, and inferring consent would "thwart" the Wiretap Act's "strong purpose to protect individual privacy." *Watkins*, 704 F.2d at 582.

Google also contends that "[n]othing in [its] disclosures regarding Analytics states or suggests that a user's browser mode affects Analytics' receipt of the Data." MTD at 12 (citing Exs. 21–23, 26). But any such omission from Google's disclosures actually supports Plaintiffs' argument, not Google's: the purported disclosures did ***not*** inform the websites that visitors in private browsing mode would continue to have their communications intercepted, contrary to Google's other representations to users and websites. *See* FAC ¶¶ 75-76, 83.

Finally, Google claims that it is "implausible" for Plaintiffs to allege that websites expected Google to refrain from intercepting "private browsing" communications. MTD at 12. Not so. In fact, Google represents to websites that they ***must*** receive consent from their users in order for those users to be tracked through Google Analytics. *See, e.g.*, MTD Ex. 23 at 1. It is therefore entirely *plausible* that websites would believe that Google would honor its visitors' use of "private browsing" by not intercepting those visitors' communications with the website. Google's actions speak much louder than its brief. After this lawsuit was filed, Google began testing a "Consent Mode" to help websites distinguish between sessions where the website has indeed received user consent to Google Analytics and other Google services. FAC ¶ 73.

B. Consent Is Irrelevant Because Google Intercepted the Private Browsing Communications with the Intent to Commit a Criminal or Tortious Act

Google's motion should in any case be denied as to the Wiretap Act claim because of the unlawful-purpose exception to the consent defense. Consent is *not* a defense where the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). As detailed in the FAC, that unlawful-purpose exception applies here. FAC ¶¶ 154-65.

Here, Google's "purpose" was to associate data from the intercepted private browsing communications with preexisting user profiles, enriching those profiles; to sell these profiles to advertisers; and to send targeted advertisements, based on the intercepted communications. FAC

¶¶ 91, 93, 115, 160-64. These subsequent acts by Google all occurred ***after*** Google's initial interception, constituting violations of other laws. FAC ¶¶ 154-65, 233. Google does *not* dispute that a post-interception violation of these laws would qualify for the unlawful-purpose exception. Instead, Google disputes the facts: Google contends that it does not correlate private browsing communications with individual users (MTD at 19-20). Those contentions are contrary to Plaintiffs' allegations (FAC ¶¶ 92-112) and cannot be resolved on a motion to dismiss.

1. The FTC Consent Decree

In 2010, the FTC charged Google with violating its privacy promises, and Section 5 of the Federal Trade Commission Act ("FTCA"), in connection with the launch of its social network, Google Buzz. FAC ¶ 25. The FTC and Google entered into a consent decree (the "FTC Consent Decree") which ordered Google to obtain "express affirmative consent" from each user "prior to any new or additional sharing" of that user's information that is "a change from stated sharing practices in effect at the time [Google] collected such information." FAC ¶¶ 25-26, 158.

When Google collected data from users in private browsing mode, Google intended to (and later did) share that data with third parties, including advertising customers, in a manner that violated the FTC's Decree. FAC ¶¶ 159-60. That sharing was a subsequent act by Google (occurring *after* the interception) which violated the Decree because it contradicted Google's "stated sharing practices" without first obtaining users' "express affirmative consent." *Id.*

These violations of the FTC Consent Decree, which occurred after the interceptions, trigger the "criminal or tortious act" exception to the consent defense. *Cf. Hameed-Bolden v. Forever 21 Retail, Inc.*, No. CV1803019SJOJPRX, 2018 WL 6802818, at *8 (C.D. Cal. Oct. 1, 2018) (holding that a claim for "unlawful" business practices under the UCL can be predicated on an FTCA violation); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *33 (N.D. Cal. May 27, 2016) (Koh, J.) (addressing a UCL claim predicated on a FTCA violation).

2. The California Consumer Privacy Act ("CCPA")

Google's subsequent use of the intercepted communications also violated the CCPA, which similarly protects Plaintiffs' browsing data. The CCPA required Google to disclose its data

collection "at or before the point of collection" and forbade Google from "us[ing] personal information collected for additional purposes without providing the user with notice consistent with this section." Cal. Civ. Code § 1798.100(b). "Personal information" includes private browsing communications. Cal. Civ. Code § 1798.140(o)(1). Here, Google intercepted the private browsing communications with the intent to (and later did) "use" the data "for additional purposes without providing the consumer with notice." FAC ¶¶ 52, 156-57. Google associated the data with users' preexisting profiles, enriching those profiles; sold it to advertisers; and used the data to direct targeted advertisements, based on the data, to Plaintiffs and their devices. FAC ¶¶ 91, 93, 115, 160-64. This violation of the CCPA is a tortious act. *See* Cal. Civ. Code § 1798.155.

3. The Comprehensive Computer Data Access and Fraud Act ("CDAFA")

The CDAFA makes it a "public offense" to "[k]nowingly access[] and *without permission* take[], cop[y], or *make[] use of* any data from a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2) (emphasis added); *see id.* § (d)(1) (violation of (c)(2) is a felony). Google's copying (interception) of Plaintiffs' private browsing communications and scraping for other browser information, in and of itself, violated this statute. *See infra* Section III. Moreover, Google's *subsequent* use of the communications constituted additional, independent violations of the CDAFA. Google "ma[d]e use of [the] data" in a manner for which it lacked permission, namely: associating the data with users' preexisting profiles; selling it to advertisers; and using it to direct targeted advertisements, based on the data, to Plaintiffs and their devices. FAC ¶¶ 91, 93, 115, 160-64. Google's subsequent "use" of the data, in violation of the CDAFA, satisfies Section 2511(2)(d)'s unlawful-purpose exception. *See In re Maxim Integrated Prod., Inc.*, No. 12-244, 2013 WL 12141373, at *15 (W.D. Pa. Mar. 19, 2013) (holding that a violation of the Computer Fraud and Abuse Act "is sufficient to satisfy the requirements of the crime-tort exception").

4. Intrusion Upon Plaintiffs' Seclusion and Constitutional Right to Privacy

Google's subsequent use of Plaintiffs' private browsing communications also constituted separate and independent torts in the form of intrusion upon seclusion and a violation of Plaintiffs' constitutional right to privacy. *See infra* Section IV. "[S]ubsequent disclosure of the contents of

the intercepted conversations for the alleged purpose of *further* invading the [Plaintiffs'] privacy" is a tortious act that satisfies the Section 2511(2)(d) unlawful-purpose exception. *Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016). Plaintiffs' private browsing activity may reveal their sexual interests, dating preferences and political or religious views, among other types of "sensitive" information and "habits" they desire to keep private. FAC ¶ 162; *Davis*, 956 F.3d at 604. Google further intrudes upon Plaintiffs' right to privacy when it sells this information to advertisers and uses the information to send targeted advertisements to Plaintiffs and to Plaintiffs' devices. FAC ¶¶ 115, 163-64.

C. The "Ordinary Course of Business" Exception Does Not Apply

Google's final defense to Plaintiffs' Wiretap Act claim is the "ordinary course of business" exception. MTD at 13. That exception does not apply for two independent reasons. *First*, Plaintiffs allege that Google's conduct violated Google's own privacy policies and disclosures. FAC ¶¶ 42-59. Those violations are dispositive: The fact "that Google violated Google's own agreements and internal policies with regard to privacy . . . preclude[s] application of the ordinary course of business exception." *Gmail*, 2013 WL 5423918, at *8.

Second, Google has not carried its burden of showing that its interception of users' communications "facilitates the transmission of the communication at issue" or is "an instrumental part of the transmission." *Gmail*, 2013 WL 5423918, at *8. Plaintiffs allege that Google's interception neither "facilitates" nor is an "instrumental part of" the transmission from the user's computer to the website. FAC ¶¶ 63-66. Rather, Google's code causes the user's computer to generate an additional duplicated and enriched transmission, scraped from the user's computer to Google's servers. *Id.* That additional transmission is neither "part of" nor "instrumental" to the communication between the user's computer and the website. *Id.*

Rather than even attempt to meet the narrow confines of this exception, Google contends that the "underlying service" Google is providing is not the communication between the user and the website, but rather Google's provision of analytics to websites, and that Google's interception facilitates *that other* analytics service. MTD at 13. But if Google's wholesale reinterpretation of

the ordinary-course-of-business exception were adopted, then this exception would swallow the rule. Nearly every interceptor of communications will be able to claim that the interception was useful to facilitate some *other*, unrelated service that the interceptor wished to provide to someone. That is why this Court, in *Gmail*, rejected Google's proposed reinterpretation of the ordinary-course-of-business exception. 2013 WL 5423918, at *9 ("Congress did not intend to allow electronic communication service providers unlimited leeway to engage in any interception that would benefit their business models, as Google contends.").[7]

II. Plaintiffs State Claims Under the California Invasion of Privacy Act

Google's interception of Plaintiffs' private browsing communications also violated sections 631 and 632 of the California Invasion of Privacy Act ("CIPA"). FAC ¶¶ 218-29. Here again, Google's principal defense is that Plaintiffs and the websites consented to Google's interceptions. CIPA requires that *all* parties consent. *Gmail II*, 2016 WL 5339806, at *16; Cal. Penal Code §§ 631(a), 632(a). As explained above, Google cannot prevail on the consent argument, because no parties consented. Other than the "consent" argument, Google offers no other basis to dismiss Plaintiffs' Section 631 claim. *See* MTD at 14.

As to Plaintiffs' Section 632 claim, Google contends that Plaintiffs' communications do not qualify as "confidential" for purposes of Section 632(a). MTD at 14. A communication qualifies as "confidential under section 632 if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 776-77 (2002). The test for "confidential" does *not* require the plaintiff to show an "additional belief that the information would not be divulged [by the defendant] at a later time to third parties." *Mirkarimi v. Nevada Prop. 1 LLC*, No. 12CV2160-BTM-DHB, 2013 WL 3761530, at *2 (S.D. Cal. July 15, 2013). The plaintiff only needs to show a reasonable "expectation that the conversation was not being simultaneously disseminated to an unannounced

[7] *See also S.D. v. Hytto Ltd.*, No. 18-CV-00688-JSW, 2019 WL 8333519, at *9 (N.D. Cal. May 15, 2019) (holding that the ordinary-course-of-business exception must be construed "narrowly" and rejecting the defendant's reliance on the exception because the defendant "failed to explain why it would be difficult or impossible to provide its service without the objected-to-interception").

second observer," when the communication occurred. *Id.*; *see also Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1397 (2011) ("[T]hat plaintiffs may have known the information discussed in their phone calls would be disclosed to other [of defendant's] employees does not mean the plaintiffs had no reasonable expectation that their telephone conversation[s] were not being secretly overheard.").

Here, Plaintiffs have alleged that the communications were "confidential." Plaintiffs allege that they expected that their private browsing communications were not being overheard by Google. FAC ¶¶ 61, 214, 227; *Flanagan*, 27 Cal. 4th at 776; *Mirkarimi*, 2013 WL 3761530, at *2. Those expectations were reasonable because Google never disclosed its interception and instead promised privacy. *See, e.g.*, FAC ¶ 42 ("[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used."). And users would have certainly expected to be confidential the additional information that Google also scrapes from the browser.

Google contends that "California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632," but Google cites just one California state court decision: *People v. Nakai*, 183 Cal. App. 4th 499 (2010). In *Nakai*, the communications at issue were "chat" messages sent through Yahoo. *Nakai* does not control here because Yahoo's privacy policy stated Yahoo could "archive" and "save" these chat messages. *Id.* at 518. Here, Plaintiffs pled the opposite: Google's disclosures told its users that their private browsing communications were private and would "not be saved" by Google. FAC ¶ 42.

The federal cases Google cites are likewise inapposite. Most of them did not even consider web browser communications.[8] Only one of Google's federal authorities, the *New Moosejaw* decision, addressed web browser communications. *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019). In *New Moosejaw*, the website at issue was in the business of selling clothing to consumers. The communications at issue were requests (clicks) from the browser to view details about various items of clothing. *Id.* at *1. The *New Moosejaw* court held

[8] All of Google's cases here lead back to *Nakai*, which turned on the fact that Yahoo's chat service could "archive" and "save" any messages. This case involves the opposite representation, namely that Plaintiffs' private browsing was private. FAC ¶ 42.

that "these particular internet communications" were not "confidential." *Id.* at *3. Here, by contrast to *New Moosejaw*, Plaintiffs have alleged that Google intercepted their communications with thousands of different websites—including dating websites, political websites, and many other highly sensitive and confidential websites, while private browsing mode was enabled. FAC ¶ 162. The reasoning from *New Moosejaw* does not apply.

III. Plaintiffs State a Claim Under the CDAFA

Plaintiffs allege that Google violated the CDAFA (FAC ¶¶ 230-38), which creates civil liability for anyone who "[k]nowingly access[es] and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2). Plaintiffs detail how Google acted without permission, including by creating "hidden" software code that "sends secret instructions back to the user's browser, without alerting the user" and "render[ing] ineffective any barriers users may wish to use to prevent access to their information, including by browsing in Incognito mode." FAC ¶¶ 5, 65-66.

First, Google's "consent" arguments (MTD at 16-17) fail for the reasons explained above.

Second, Google's "term of use" arguments (MTD at 16) are irrelevant. Citing *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780 JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010), Google argues that there can be no CDAFA liability where a defendant just "violated a contractual term of use." MTD at 16. This argument is irrelevant, because Plaintiffs' CDAFA claim is not based on a violation of a "terms of use" document. Instead, Plaintiffs allege that Google acted "without permission" by secretly and without notice taking and using their data. *Power Ventures* provides no basis for Google's motion.[9]

Third, Google's contention that there must be some "circumvention" of a "technical or code-based barrier" (MTD at 16) is incorrect. In 2015, the Ninth Circuit clarified that, unlike the Computer Fraud and Abuse Act, the CDAFA "does not require *unauthorized* access. It merely

[9] The *Power Ventures* reasoning is based on constitutional concerns that do not apply here, where notice could hinge solely on compliance with a website's terms of use such that the website owner could define the scope of criminal liability. 2010 WL 3291750, at *11-12. Google cannot complain that it lacked notice or is being subject to liability based on its own terms of use.

requires *knowing* access." *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015) (emphasis in original). The "term 'access' as defined in the [CDAFA] includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *Id.* Citing *Christensen*, numerous courts have rejected Google's contention and ruled that circumvention is *not* required. *See, e.g.*, *Henry Schein, Inc. v. Cook*, 2017 WL 783617, at *5 (N.D. Cal. Mar. 1, 2017).

Fourth, even were the Court to apply some circumvention requirement, contrary to *Christensen*, Plaintiffs' factual allegations are sufficient. Google secretly embedded software code that caused Plaintiffs' browsers to send Google a secret copy of the user-website GET request, and additional data scraped from the browser, rendering ineffective Plaintiffs' efforts to prevent access to their information by initiating a private browsing mode. FAC ¶¶ 5, 65-66. That is sufficient to state a CDAFA claim. *In re Carrier IQ*, 78 F. Supp. 3d 1051, 1101 (N.D. Cal. 2015) (denying motion to dismiss CDAFA claim where plaintiffs alleged that "hidden" software transmitted data without notice or any way to stop the functionality); *see also Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1073-74 (N.D. Cal. 2018) (denying motion to dismiss CDAFA counterclaim where defendants alleged "hidden" software exceeded authorized use).

Fifth, Google's reliance on *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110 (N.D. Cal. 2020) (Koh, J.) is misplaced. There, the plaintiffs asserted both CFAA and CDAFA claims, and the plaintiffs did not cite (and the Court therefore did not reference) the Ninth Circuit's *Christensen* decision. *Id.* at 131 (citing pre-*Christensen* case law suggesting elements of CFAA and CDAFA claims "do not differ materially") (citation omitted). The Court found that that the plaintiffs' "boilerplate" allegations were insufficient, because their assertion that Apple acted without permission was just a "legal conclusion" unsupported by factual allegations. *Id.* at 123, 132. Here, by contrast, Plaintiffs include detailed factual allegations establishing that Google acted without permission. FAC ¶¶ 41-66, 73-77, 84-88, 148-50, 168-70, 173-75, 178-80, 183-85.

Sixth, even setting aside whether Google had permission to access Plaintiffs' private browsing data (Google did not), Google's argument would still fail because the CDAFA also

forbids Google's "use" of that data without permission. Cal. Penal Code § 502(c)(2) (liability both for "takes" and "makes use"); *Christensen*, 828 F.3d at 789 ("[CDAFA's] focus is on unauthorized taking or use of information."). Here, Plaintiffs did not give their permission for Google to associate the private browsing data with individual user profiles, to sell it to third parties, or to use it to send targeted advertisements to Plaintiffs and Plaintiffs' devices. FAC ¶¶ 91, 93, 115, 157-64, 232-34. These "use" allegations are separate and independent violations of the CDAFA. *See Cook*, 2017 WL 783617, at *5 (N.D. Cal. Mar. 1, 2017) ("[S]ubsequently misusing the information obtained constitutes a section 502 violation.").

IV. Plaintiffs State Constitutional and Common Law Privacy Claims

Plaintiffs have also stated claims for intrusion upon seclusion and invasion of privacy. FAC ¶¶ 239-66. "Because of the similarity of the tests, courts consider the[se] claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Davis*, 956 F.3d at 601. Plaintiffs have met both elements.[10]

A. Plaintiffs Had a Reasonable Expectation of Privacy

Plaintiffs have alleged a reasonable expectation of privacy, both because of the highly sensitive nature of their private browsing communications *and* because Google led them to believe that it would not intercept these communications. FAC ¶¶ 3-4, 41-43, 53, 146, 162, 233.

Plaintiffs' allegations are consistent with and sufficient under the Ninth Circuit's *Davis* decision. *Davis* addressed the same kind of web-browsing communications at issue in this case—GET requests sent from a user's browser to the website, telling the website what content to display. 956 F.3d at 607; FAC ¶¶ 63, 208. Like Google, Facebook received copies of the GET requests users sent to third-party websites. 956 F.3d at 607; FAC ¶ 63. Like Google, Facebook obtained these copies because Facebook's embedded code caused the users' browsers to generate copies of the user-website GET requests and transmit them to Facebook "through a separate, but

[10] Google's consent defense also fails in connection with these claims. *See supra* Section I.A; *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1074 (N.D. Cal. 2016) (denying summary judgment on basis that jury could find that privacy policy provisions "do not explicitly address—and thus do not obtain knowing consent for–" the challenge practices).

simultaneous, channel in a manner undetectable by the user." 956 F.3d at 596, 608; FAC ¶¶ 64, 213. Like Google, Facebook "compile[d] these browsing histories into personal profiles which are sold to advertisers to generate revenue." 956 F.3d at 596; FAC ¶¶ 91-112, 115, 160-64. Like Google, Facebook first "set an expectation" with its users that this data would not be collected under certain circumstances (when users logged off Facebook), "but then collected it anyway." 956 F.3d at 602; FAC ¶¶ 3-4, 41-43.

The Ninth Circuit held that the plaintiffs had a reasonable expectation of privacy in their browsing communications, explaining: "the allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits prevent us from concluding that the Plaintiffs have no reasonable expectation of privacy." 956 F.3d at 604. The plaintiffs' privacy expectation was also reasonable because of Facebook's "allegedly surreptitious and unseen" method of collecting the GET requests—a method that is very similar to Google's practices at issue in this case. *Id.* at 603. Google has likewise "compiled highly personalized profiles from sensitive browsing histories and habits" after "set[ting] an expectation" that this data would not be collected during private browsing sessions. *Id.* at 602, 604. That is abundantly sufficient. *See also In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293-95 (3d Cir. 2016) (holding, under analogous New Jersey law, that users had a reasonable expectation of privacy when Viacom promised that it would not collect information but then did); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 151 (3rd Cir. 2015) (holding, under California law, that users had a reasonable expectation of privacy in their browsing histories).

Google's contention that Plaintiffs have only "conclusorily" alleged that Google associates the data with users' Google profiles (MTD at 19) is meritless. Plaintiffs include detailed allegations regarding that association with profiles (FAC ¶¶ 89-112), and discovery is required to resolve this factual dispute. *See Manzarek*, 519 F.3d at 1031. In any event, Plaintiffs' expectation of privacy was reasonable regardless of whether Google subsequently associated the intercepted data with users' profiles. Under *Davis*, "the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it

anyway." 956 F.3d at 603. Indeed, Plaintiffs' expectation of privacy was even higher here than in *Davis*, in which the plaintiffs used a normal (non-private) browsing mode and were merely attempting to shield their browsing activity from Facebook. 956 F.3d at 602-03. Here, *all* of the intercepted communications were sensitive, as shown by Plaintiffs' decision to enable private browsing mode. Users enable "private browsing" in order to shield their dating activity, sexual interests, or political or religious views, among other sensitive information. FAC ¶ 162.

Finally, in light of *Davis*, Google does not (and cannot) cite any authority to support its contention that "web browsing data that is not associated with a particular user or their device after the session is closed, cannot support [a] privacy claim[]." MTD at 20-21. Each case Google cites for this proposition came before *Davis* and is also factually inapposite.[11]

B. Google's Conduct Was "Highly Offensive"

Plaintiffs have also alleged facts establishing that Google's conduct was "highly offensive," particularly insofar as it collected extremely personal information after users enabled

[11] *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) (Koh, J.) only rejected the claim that plaintiffs had a reasonable expectation of privacy in the "limited information" LinkedIn collected, "a user's browsing history among LinkedIn profiles." *Id.* at 1025, 1030. The data here concerns private communications far beyond browsing a single website's professional profiles. *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) (Koh, J.) dismissed the Wiretap Act Claim because the intercepted data was not the "content" of any communication; it was "information about the identities of parties to a communication." *Id.* at 1061. The GET requests at issue in this case contain far more "content," including specific content displayed by the website. *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 974-75 (N.D. Cal. 2014), involved an amendment of Google's privacy policy, which is inapposite here. *Moreno v. San Francisco Bay Area Rapid Transit District*, No. 17-CV-02911-JSC, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) turned on the fact that the plaintiff was "on notice that [the defendant] would be accessing the information." Here, Plaintiffs allege just the opposite. *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (Koh, J.) held plaintiffs' allegations were "conclusory" and "merely allege[d] that [their] emails were 'private.'" *Id.* Here, the communications were private because *private* browsing mode was enabled. FAC ¶ 162.

The four cases Google cites in footnote 16 (MTD at 22) are even further afield. In *Yunker v. Pandora Media, Inc.* the plaintiff failed to even allege that the defendant intercepted the communications at issue. No. 11-CV-03113 JSW, 2013 WL 1282980, at *7 (N.D. Cal. Mar. 26, 2013). *Gonzales v. Uber Technologies, Inc.* concerned Lyft drivers' geolocation data, which is automatically shared with prospective riders. 305 F. Supp. 3d 1078, 1092 (N.D. Cal. 2018). *Belluomini v. Citigroup, Inc.* rejected a claim that a bank violated the account holder's right to privacy merely by giving the account holder's contact information to a third-party. No. CV 13-01743 CRB, 2013 WL 3855589, at *7 (N.D. Cal. July 24, 2013). And *Folgelstrom v. Lamps Plus, Inc.* rejected a claim that a retailer invaded the plaintiff's right to privacy by asking for his zip code during credit card transactions. 195 Cal. App. 4th 986, 992, 125 (2011).

private browsing and "using duplicitous tactics." *In re Nickelodeon*, 827 F.3d at 295. Google's arguments are the same arguments that the Ninth Circuit rejected in *Davis*, 956 F.3d at 606, and they should likewise be rejected in this case. Google's "surreptitious" interception targets private browsing of thousands of different websites, including dating websites, political websites, and myriad highly sensitive websites. *Davis*, 956 F.3d at 606; FAC ¶ 162. A user enables private browsing mode to prevent others, including both family and Google, from finding out that he or she is viewing these kinds of sites and the specific content therein. FAC ¶¶ 3, 41-42, 162. Google touted private browsing mode as a safe space to do all these things but then intercepted Plaintiffs' private-browsing communications anyway, and thereafter used that data to profile and target users. FAC ¶¶ 1-4, 41-42, 91, 93, 115, 160-64; *see Davis*, 956 F.3d at 606 (holding that "allegations of surreptitious data collection" suffice for highly offensive conduct). Again, Google's conduct is even more offensive than the conduct in *Davis*, where the plaintiffs were not using a private browsing mode. The fact that Google employees recognized that Google's privacy disclosures are a "mess" (FAC ¶ 36) also suggests the conduct is highly offensive. *See Davis*, 956 F.3d at 606.

Google contends that its conduct cannot be "highly offensive" because its "routine" interceptions of Plaintiffs' private browsing communications "served a legitimate commercial purpose." MTD at 22. But none of the cases cited by Google, applying the (purported) "legitimate commercial purpose" standard, involved *private* browsing communications.[12] The Third Circuit (applying California law) has already rejected Google's argument, and held that the "routine" nature of interceptions is an irrelevant "smokescreen." *In re Google Inc. Cookie*, 806 F.3d at 150. "[U]sers are entitled to deny consent, and they are entitled to rely on the public promises of the

[12] *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 817, 830 (N.D. Cal. 2020) found that the plaintiffs did not have a reasonable expectation of privacy for communications mistakenly picked up by Google Assistant. Here, Google intentionally "picked up private [browsing] communications." *Id.* at 817. Google's reliance on *In re Nickelodeon,* 827 F.3d at 294 is also misplaced. The court distinguished Google's conduct in that case from Viacom's, because Viacom "created an expectation of privacy on its websites" by promising users that it would not collect children's data. *Id.* at 292. *In re Google, Inc. Privacy Policy*, 58 F. Supp. 3d at 981 is inapposite. The plaintiffs' complaint was that Google changed its privacy policy after the plaintiffs had already purchased Android devices in reliance on the old privacy policy. Here, by contrast, Plaintiffs allege that Google has violated its current Privacy Policy, not an old one.

companies they deal with." *Id* at 151. As in *Davis*, Plaintiffs' allegations of "surreptitious" data collection are sufficient. 956 F.3d at 606.[13]

V. Plaintiffs' Claims Are Timely

Each wrongful interception of data, and each subsequent use of that data, is a separate violation that has its own statute of limitations. For Wiretap Act claims, which require plaintiffs to bring an action within two years after the claimant "first has a reasonable opportunity to discover the *violation*," the Ninth Circuit recently clarified that "each interception is a discrete *violation*." *Bliss v. CoreCivic, Inc.*, No. 19-16167, 2020 WL 6279679, at *3-4 (9th Cir. Oct. 27, 2020) (emphasis added) (citing 18 U.S.C. § 2520(e)). The same logic applies to Plaintiffs' CIPA claims, which likewise refer to "'communication' in the singular." *Id.* at *3; Cal. Penal Code § 631(a) (proscribing the unauthorized interception of "any message, report, or communication"); *id.* § 632(a) (proscribing the interception of a "confidential communication"). Similarly, CDAFA's statute of limitations is pegged to "the date of the *act* complained of, or the date of the discovery of the damage, whichever is later." Cal. Penal Code § 502(e)(5) (emphasis added). The same rule should apply for Plaintiffs' intrusion upon seclusion and constitutional claims. Accordingly, Plaintiffs have stated claims for all of Google's conduct that occurred, at the very least, during the statute-of-limitations period prior to the filing of the original Complaint.

In any event, the statutes of limitations have been tolled under: (1) the fraudulent concealment doctrine; and (2) the delayed discovery doctrine. "[A] statute of limitations may be tolled if the defendant fraudulently concealed the existence of a cause of action in such a way that the plaintiff, acting as a reasonable person, did not know of its existence." *In re Animation Workers Antitrust Litig.*, 123 F. Supp. 3d 1175, 1194 (N.D. Cal. 2015) (Koh, J.) (citation omitted). This is what Plaintiffs allege happened here. FAC ¶¶ 42, 52, 146 (listing numerous false statements by

[13] *See also Nickelodeon*, 827 F.3d at 292 ("Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses."); *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) ("[R]outine data collection practices may be highly offensive if a defendant disregards consumers' privacy choices while simultaneously holding itself out as respecting them."); *In re Google Assistant*, 457 F. Supp. 3d at 830 (noting that "courts have repeatedly found the surreptitious recording of a plaintiff's conversations or activity to constitute an actionable intrusion").

Google concerning private browsing, including the dates, speakers, and contents). At a minimum, these were "misleading partial disclosures," tolling the statutes of limitations. *In re Animation Workers*, 123 F. Supp. 3d at 1203. "The fact-intensive nature of fraudulent concealment makes disposition of that issue 'generally inappropriate' on the pleadings." *In re Lithium Ion Batteries Antitrust Litig.*, No. 13-MD-2420 YGR, 2014 WL 309192, at *16 (N.D. Cal. Jan. 21, 2014).

For similar reasons, the statutes of limitations were also tolled under the delayed discovery doctrine. "In California, the discovery rule postpones accrual of a claim until the plaintiff discovers, or has reason to discover, the cause of action." *Cover v. Windsor Surry Co.*, No. 14-CV-05262-WHO, 2015 WL 4396215, at *4 (N.D. Cal. July 17, 2015) (citation omitted). Google criticizes Plaintiffs for failing to ask Google directly whether it was intercepting their private browsing communications. MTD at 24. That argument "puts the cart before the horse, however, as Plaintiffs were not obligated to investigate their claims *until* Plaintiffs had reason to suspect the existence of their claims." *In re Animation Workers*, 123 F. Supp. 3d at 1204. The two 2018 articles cited in the FAC are not "evidence" of the particular misconduct at issue here because they do not suggest that Google was intercepting communications from users in private browsing mode (nor does Google claim otherwise). MTD at 24 (citing FAC ¶¶ 106, 109). Google's reliance on *Plumlee v. Pfizer, Inc.*, is therefore misplaced. *See* No. 13-CV-00414-LHK, 2014 WL 695024, at *8 (N.D. Cal. Feb. 21, 2014) (Koh, J.). Finally, the limitations periods for the CIPA, constitutional, and common law privacy claims are two years, not one. *See* Cal. Civ. Proc. Code § 335.1.[14]

VI. CONCLUSION

For the foregoing reasons, this Court should deny Google's Motion to Dismiss. If this Court disagrees, any dismissal should be without prejudice and with leave to amend.

[14] The cases Google cites can all be traced back to *Cain v. State Farm Mutual Auto. Ins. Co.*, 62 Cal. App. 3d 310 (1976), which held that privacy claims are governed by the one-year statute of limitations for personal injury actions. The statute was codified at § 340(c). In 2003, that provision was moved to § 335.1 and the limitations period was extended to two years. Courts now apply that two-year limitations period to privacy claims. *See Quan v. Smithkline Beecham Corp.*, 149 F. App'x 668, 670 (9th Cir. 2005); *see also Wilson v. City of Oakland*, No. C-11-05377 DMR, 2012 WL 669527, at *3 (N.D. Cal. Feb. 29, 2012); *O'Shea v. Cty. of San Diego*, No. 19-CV-1243-BAS-BLM, 2020 WL 2767357, at *2 (S.D. Cal. May 28, 2020); *Saling v. Royal*, No. 2:13-CV-1039-TLN-EFB, 2015 WL 5255367, at *3 (E.D. Cal. Sept. 9, 2015).

Dated: November 18, 2020

SUSMAN GODFREY L.L.P.

By: /s/ Amanda Bonn

Amanda Bonn (CA Bar No. 270891)
abonn@susmangodfrey.com
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100

Mark C. Mao (CA Bar No. 236165)
mmao@bsfllp.com
Sean Phillips Rodriguez (CA Bar No. 262437)
srodriguez@bsfllp.com
Beko Rebitz-Richardson (CA Bar No. 238027)
brichardson@bsfllp.com
Alexander Justin Konik (CA Bar No. 299291)
akonik@bsfllp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery Street, 41st Floor
San Francisco, CA 94104
Telephone: (415) 293 6858
Facsimile (415) 999 9695

James W. Lee (*pro hac vice*)
jlee@bsfllp.com
Rossana Baeza (*pro hac vice*)
rbaeza@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Street, Suite 2800
Miami, FL 33130
Telephone: (305) 539-8400
Facsimile: (305) 539-1304

William Christopher Carmody (*pro hac vice*)
bcarmody@susmangodfrey.com
Shawn J. Rabin (*pro hac vice*)
srabin@susmangodfrey.com
Steven Shepard (*pro hac vice*)
sshepard@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (212) 336-8330

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice*)

rmcgee@forthepeople.com
Michael F. Ram (*pro hac vice*)
mram@forthepeople.com
Ra O. Amen (*pro hac vice*)
ramen@forthepeople.com
MORGAN & MORGAN, P.A.
201 N Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4736

Attorneys for Plaintiffs